PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-036561
(43)Date of publication of application : 09.02.2001

(51)Int.Cl. H04L 12/46
H04L 12/28
H04L 12/56
// H04L 9/32

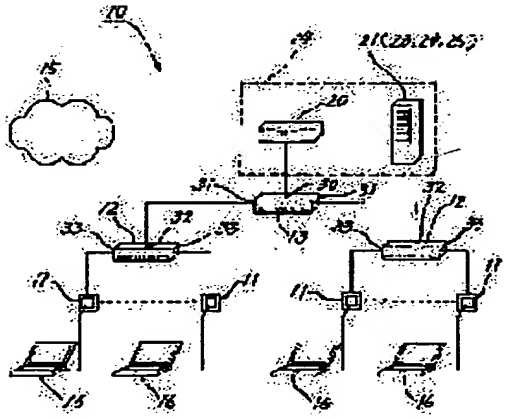
(21)Application number : 11-201525
(22)Date of filing : 15.07.1999

(71)Applicant : MARUYAMA SHIN
ASANO YOSHIO

(72)Inventor : MARUYAMA SHIN
ASANO YOSHIO
TSUJI HITOSHI
FUJII YASUO
NAKAMURA JUNICHI

(54) TCP/IP NETWORK SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve security without revising a DHCP(dynamic host configuration protocol) and the hardware and the software of a terminal in a TCP/IP network system using a DHCP server.
SOLUTION: The TCP/IP network system 10 is provided with hubs 12, 13 with a plurality of ports to which a terminal 16 is connected, a router 20 connected to the hubs 12, 13 and an external network 15, and a server 21 that is connected to the router 20 to serve various services to the terminal 16. The server 21 is provided with a DHCP server 23, the hubs 12, 13 are switching hubs that can section the network logically or physically, and each information wall socket 11 is set so as to belong to the sectioned network by the information wall socket 11 and the router 20.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００１－３６５６１
（Ｐ２００１－３６５６１Ａ）
(43)公開日　平成13年2月9日(2001.2.9)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｈ０４Ｌ	12/46		Ｈ０４Ｌ	11/00	３１０　Ｃ	5J104
	12/28			11/20	１０２　Ｄ	5K030
	12/56			9/00	６７５　Ｄ	5K033
// Ｈ０４Ｌ	9/32					9A001

審査請求　未請求　請求項の数６　ＯＬ　（全８頁）

(21)出願番号　特願平11-201525

(22)出願日　平成11年7月15日(1999.7.15)

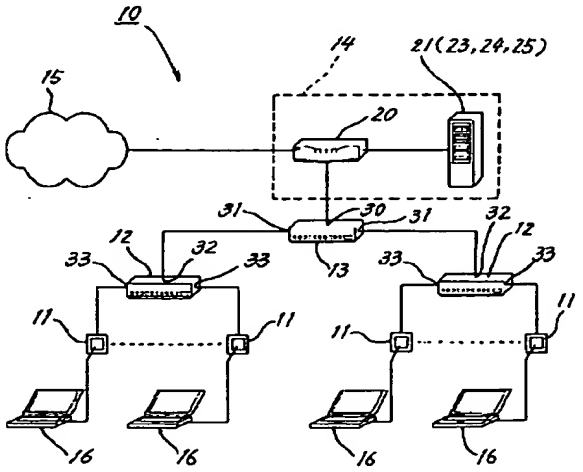
特許法第30条第1項適用申請有り　平成11年5月11日～7月13日、丸山伸、浅野善男が京都大学附属図書館3階、総合情報メディアセンター図書館サテライト教室でＴＣＰ／ＩＰネットワークの試験を行う

(71)出願人　599099652
丸山　伸
大阪府豊中市新千里東町2－4　D6－401
(71)出願人　599099663
浅野　善男
滋賀県草津市南笠町448－1－1428
(72)発明者　丸山　伸
大阪府豊中市新千里東町2－4　D6－401
(72)発明者　浅野　善男
滋賀県草津市南笠町448－1－1428
(74)代理人　100066728
弁理士　丸山　敏之　（外2名）

最終頁に続く

(54)【発明の名称】ＴＣＰ／ＩＰネットワークシステム

(57)【要約】
【課題】　DHCPサーバを用いたTCP/IPネットワークシステムにおいて、DHCPプロトコルや、端末機におけるハードウェアおよびソフトウェアに変更を加えることなく、セキュリティを向上させる。
【解決手段】　本発明のTCP/IPネットワークシステム10は、端末機16が接続される複数のポートを具えるハブ12、13と、該ハブ12、13及び外部ネットワーク15に接続されるルータ20と、該ルータ20に接続され、端末機16に各種サービスを提供するサーバ21とを具える。サーバ21は、DHCPサーバ23を具えており、前記ハブ12、13は、ネットワークを物理的又は論理的に区分化できるスイッチングハブであり、各情報コンセント11が、該情報コンセント11とルータ20からなる区分化されたネットワークに所属するように設定される。



1

【特許請求の範囲】

【請求項１】　ＴＣＰ／ＩＰプロトコルを利用したネットワークシステムであって、

端末機が接続される複数のポートを具えるハブと、該ハブ及び外部のネットワークに接続されるルータと、該ルータに接続され、ネットワーク上に接続された端末機に各種サービスを提供するサーバとを具えており、

該サーバは、複数のＩＰアドレスを記憶し、ネットワークに接続された端末機に、該ＩＰアドレス中の１つを割り当てるＤＨＣＰサーバを具えており、

前記ハブは、ＶＬＡＮ管理方式等、ネットワークを物理的又は論理的に区分化できるスイッチングハブであり、ハブの各ポートが、該ポートとルータからなる区分化されたネットワークに所属するように設定されているネットワークシステム。

【請求項２】　サーバは、ネットワーク利用者の認証を行なう認証サーバを具えており、ルータは、認証サーバの認証により認可されたＩＰアドレスを有する端末機から送信されるパケットのみを、区分化されたネットワークの外部に送信するように設定される、請求項１に記載のネットワークシステム。

【請求項３】　スイッチングハブは、ネットワーク利用者の認証により認可されたＩＰアドレスと、該ＩＰアドレスを有する端末機が接続されたポートのＭＡＣアドレスとの組合せを記憶しており、該端末機から送信されるパケット中に含まれる発信元のＩＰアドレスと該ポートのＭＡＣアドレスとの組合せが、記憶した組合せと異なる場合には、該パケットのルータへの送信を阻止するフィルタリング機能を有している、請求項１又は請求項２に記載のネットワークシステム。

【請求項４】　ＤＨＣＰサーバから端末機に割り当てられるＩＰアドレスは、ネットワークシステム上でのみ有効なプライベートＩＰアドレスであり、ルータは、該プライベートＩＰアドレスと、外部ネットワーク上で有効なグローバルＩＰアドレスとを対応させながら変換するＮＡＴ機能を有する、請求項１乃至請求項３の何れかに記載のネットワークシステム。

【請求項５】　ＤＨＣＰサーバは、端末機からＩＰアドレスの割当てが要求されると、要求した端末機のＭＡＣアドレスに向けて適当なＩＰアドレスを送出するように設定される、請求項１乃至請求項４の何れかに記載のネットワークシステム。

【請求項６】　スイッチングハブは、端末機が接続される部門ハブと、複数の部門ハブ及びルータが接続される中央ハブとからなる階層構造となっている、請求項１乃至請求項５の何れかにに記載のネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＴＣＰ／ＩＰ（Transmission Control Protcol / Internet Protocol）プロトコルを利用したネットワークシステム（以下、「ＴＣＰ／ＩＰネットワーク」と称する。）に関するものである。具体的には、本発明は、ＤＨＣＰサーバを用いた該ネットワークシステムにおけるセキュリティの向上に関するものである。

2

【０００２】

【従来の技術】近時、大学等の教育機関や研究機関では、不特定多数の人間が、各自の所有するノート型パーソナルコンピュータ等の端末機を用いて、構内の研究室、図書室、コンピュータ室等の様々な場所に設置された情報コンセントから構内のＬＡＮ（Local Area Network）に接続でき、該ＬＡＮからインターネット等の外部ネットワークに接続できるようになっている。このようなネットワークシステムでは、種々の端末機が使用されることから、マルチベンダの使用に適したＴＣＰ／ＩＰプロトコルが使用されている。ＴＣＰ／ＩＰネットワークの場合、ネットワークに接続された各種デバイス（以下、「ノード」と称する。）には、４バイトの数値アドレスであるＩＰアドレスが設定されており、情報を送る際には、発信元のＩＰアドレスと宛先のＩＰアドレスを含む情報パケットが送信されることにより、ノード間の情報の送受が行なわれる。

【０００３】従って、前記ＬＡＮに接続される端末機にもＩＰアドレスを設定する必要がある。しかしながら、この場合、ＬＡＮに接続し得る全ての端末機に個別のＩＰアドレスを設定する必要があり、また、該端末機の全てが同時にＬＡＮに接続されることはほぼあり得ないことから、ＩＰアドレス資源の無駄となる。そこで、このようなネットワークシステムでは、ＤＨＣＰ(Dynamic Host Configuration Protcol) プロトコルを利用して、ＬＡＮに接続された端末機に対し、適当なＩＰアドレスを自動的に割り当てるようになっている。

【０００４】図１０は、前記ＬＡＮ(90)の概要を示している。各情報コンセント(11)はハブ(91)に接続され、ハブ(91)はルータ(92)に接続され、ルータ(92)は、外部ネットワーク(15)に接続される。また、ハブ(91)には、情報コンセント(11)に接続されたコンピュータ等の端末機に各種サービスを提供する各種サーバ(93)が接続される。サーバ(93)には、複数のＩＰアドレスを記憶し、ネットワーク上に接続された端末機に、該ＩＰアドレス中の１つを割り当てるＤＨＣＰサーバ(94)が含まれる。各デバイス間は、光ケーブル、導線ケーブル等の有線、或いは、電磁波等の無線にて接続される。ユーザが端末機を情報コンセント(11)に接続して、ＩＰアドレスの割当て要求をネットワーク上に送ると、ＤＨＣＰサーバ(94)によって割り当てられたＩＰアドレスが端末機に送られる。ユーザは、該ＩＰアドレスを用いて、ＬＡＮ(90)上の資源や、外部ネットワーク(15)の資源を利用できる。

【０００５】

【発明が解決しようとする課題】このように、ＴＣＰ／

ＩＰネットワークの場合、相手先のＩＰアドレスを知ることができれば、互いに情報を送受できる。また、ＤＨＣＰサーバは、割り当てたＩＰアドレスを端末機に送る際には、ＡＲＰブロードキャストを利用するため、ネットワーク上の他の端末機は、該ＩＰアドレスを受信可能である。従って、ＤＨＣＰプロトコルを利用したＴＣＰ／ＩＰネットワークの場合、端末機は、他の端末機と容易に情報を送受できる反面、他の端末機が悪意をもって接続し攻撃してくることに対して無防備である。

【０００６】また、前述のように、不特定多数の人間が情報コンセントを利用し得る場合には、何時、誰が、何れの情報コンセントを利用したかを記録することがセキュリティの上からも重要である。このため、端末機を情報コンセントに接続する際に認証を行なって、利用者を特定し、認証により認可された利用者のみがネットワークを利用できること望ましい。しかしながら、ＤＨＣＰプロトコルには、利用者を認証するための機能が含まれていない。この問題点を解決するため、ＤＨＣＰプロトコルに認証機能を追加する作業が進行している。しかしながら、この方法では、追加した機能をサポートするために端末機におけるハードウェアおよびソフトウェアの変更が要求されることから、利用者の負担が増大しする結果となり、即座に実施可能であるとは言い難い。

【０００７】

【発明の目的】本願は、ＤＨＣＰサーバを用いたＴＣＰ／ＩＰネットワークシステムにおいて、ＤＨＣＰプロトコルや、端末機におけるハードウェアおよびソフトウェアに変更を加えることなく、セキュリティの向上を実現したネットワークシステムを提供することを目的とする。

【０００８】

【課題を解決するための手段】上記課題を解決するため、本発明は、ＴＣＰ／ＩＰプロトコルを利用したネットワークシステムであって、端末機が接続される複数のポートを具えるハブと、該ハブ及び外部のネットワークに接続されるルータと、該ルータに接続され、ネットワーク上に接続された端末機に各種サービスを提供するサーバとを具えており、サーバは、複数のＩＰアドレスを記憶し、ネットワークに接続された端末機に、該ＩＰアドレス中の１つを割り当てるＤＨＣＰサーバを具えており、前記ハブは、ＶＬＡＮ管理方式等、ネットワークを物理的又は論理的に区分化できるスイッチングハブであり、ハブの各ポートが、該ポートとルータからなる区分化されたネットワークに所属するように設定されることを特徴とする。

【０００９】また、サーバは、ネットワーク利用者の認証を行なう認証サーバを具えており、ルータは、認証サーバの認証により認可されたＩＰアドレスを有する端末機から送信されるパケットのみを、区分化されたネットワークの外部に送信するように設定されることを特徴とする。

【００１０】

【作用及び効果】上記構成のネットワークシステムにおいて、ネットワークを物理的又は論理的に区分化できるスイッチングハブを利用して、ルータとハブの各ポート間が別々に区分化されたネットワークとなるように設定される。従って、ネットワークに接続された端末機どうしは、別々の区分化されたネットワークに所属することになり、該端末機間のセキュリティが向上する。

【００１１】また、或る端末機から、該端末機が所属する区分化されたネットワークの外部、すなわち、サーバ、他の端末機または外部ネットワークにパケットを送信する場合には、必ずルータを介して行われることになる。従って、ルータが、認証サーバの認証により認可されたＩＰアドレスを有する端末機から送信されるパケットのみを、区分化されたネットワークの外部に送信するように設定されることにより、利用者がネットワークを利用するには、認証を受ける必要性が生じ、ネットワーク上のセキュリティが向上する。

【００１２】

【発明の実施の形態】以下、本発明の実施形態について説明する。図１は、本発明の実施形態であるＴＣＰ／ＩＰネットワークシステムの概要を示している。該ネットワークシステム(10)は、端末機が接続される多数の情報コンセント(11)と、該情報コンセント(11)が接続される複数の部門ハブ(12)(12)と、該部門ハブ(12)(12)が接続される中央ハブ(13)と、該中央ハブ(13)が接続され、外部ネットワーク(15)に接続される統合サーバ(14)を具える。

【００１３】統合サーバ(14)は、中央ハブ(13)および外部ネットワーク(15)に接続されるルータ(20)と、各種サーバ(21)を具える。本実施形態の各種サーバ(21)には、複数のＩＰアドレスを記憶し、情報コンセント(11)に接続された端末機(16)に、該ＩＰアドレスの中の１つを割り当てるＤＨＣＰサーバ(23)と、利用者の認証を行なう認証サーバ(24)と、各情報コンセント(11)における端末機(16)との接続または切断状況を監視する切断監視サーバ(25)が含まれる。

【００１４】前述のように、情報コンセント(11)に新たに接続された端末機(16)が、ＤＨＣＰサーバ(23)にＩＰアドレスの割当てを要求した場合、ＤＨＣＰサーバ(23)は、割り当てるべき適当なＩＰアドレスをＡＲＰブロードキャストによって送出する。この場合、該ＩＰアドレスを他の端末機(16)により傍受される可能性がある。従って、ＤＨＣＰサーバ(23)は、要求した端末機(16)が有するＭＡＣアドレスに向けて送出するように設定されることが望ましい。

【００１５】認証サーバ(24)による認証方法には、カードによる方法、暗号化された電子メールによる方法等、種々の方法が存在する。本実施形態では、端末機(16)が

ＩＰアドレスを取得した後に認証ツールを起動して、ネットワークシステム(10)を介して認証が行なわれる。この認証ツールとしては、現在の端末機(16)に標準で装備されているWebブラウザを利用することが望ましく、該Webブラウザを介して、ＣＧＩ(Common Gateway Interface)を起動させて認証を行なうことが望ましい。また、認証サーバ(24)には、通常は、利用者を特定するためのＩＤコードおよびパスワードが記憶されている。しかしながらが、該ＩＤコードおよびパスワードが外部ネットワーク(15)の或るサーバに記憶されている場合には、認証サーバ(24)は、ＮＩＳ(Network Information Service)を利用してＩＤコードおよびパスワードを照会するように設定されていれば、ＩＤコードおよびパスワードを記憶する必要はない。また、認証サーバ(24)は、前記ＩＤコードおよびパスワードの他に、該ＩＤコードの利用者に、各種サーバ(21)、外部ネットワーク(15)および他の端末機(16)のうち、どの範囲までのアクセスを認めるかを示すアクセス制限情報を記憶しておくことが望ましい。

【００１６】ルータ(20)は、認証サーバ(24)により認証された端末機(16)に割り当てられたＩＰアドレスを有する情報のみを通過させるＩＰフィルタリング機能を有する。また、本実施形態では、ＤＨＣＰサーバ(23)により割り当てられるＩＰアドレスは、このネットワークシステム(10)上でのみ有効なプライベートＩＰアドレスであり、ルータ(20)は、該プライベートＩＰアドレスと、外部ネットワーク上で有効なグローバルＩＰアドレスを対応させながら変換するＮＡＴ(Network AddressTranslation)機能を有している。また、本実施形態のルータ(20)は、端末機(16)に割り当てられたＩＰアドレスと、該端末機(16)のＭＡＣアドレスとの組合せを記憶しており、該組合せに適合しない通信を拒否する機能を有している。なお、各種サーバ(23)(24)(25)は、公知のサーバであり、ＩＰフィルタリング機能とＮＡＴ機能を有するルータ(20)も公知のものが使用される。

【００１７】中央ハブ(13)は、ルータ(20)が接続される上流ポート(30)と、部門ハブ(12)(12)とが接続される多数の下流ポート(31)を具えており、部門ハブ(12)(12)は、中央ハブ(13)が接続される上流ポート(32)と情報コンセント(11)とが接続される多数の下流ポート(33)を具えている。このように、多数の情報コンセント(11)を利用する場合は、ハブは、中央ハブ(13)および部門ハブ(12)を具えた階層構造となることが望ましい。本発明では、中央ハブ(13)および部門ハブ(12)には、ＶＬＡＮ管理方式の設定が可能なスイッチングハブが使用される。この場合、部門ハブ(12)は、各情報コンセント(11)に接続される下流ポート(33)に対して、ＶＬＡＮグループを設定できると共に、中央ハブ(13)に接続される上流ポート(32)に対して、設定されたＶＬＡＮグループの全てを設定できる必要がある。同様に、中央ハブ(13)は、各部門ハブ(12)に接続される下流ポート(31)に対して、部門ハブ(12)にて設定されたＶＬＡＮグループの全てを設定できると共に、ルータ(20)に接続される上流ポート(30)に対して、全ての部門ハブ(12)にて設定されたＶＬＡＮグループの全てを設定できる必要がある。すなわち、中央ハブ(13)および部門ハブ(12)に使用されるスイッチングハブには、単一のポートに複数のＶＬＡＮグループを設定できる必要がある。このようなスイッチングハブとしては、IEEE802.1Q、MultiVLAN、またはCisco社の提案によるISCPに準拠したスイッチングハブが挙げられる。

【００１８】本実施形態では、部門ハブ(12)は、端末機(16)が情報コンセント(11)を介して接続された下流ポート(33)のＭＡＣアドレスと、該端末機(16)に対してＤＨＣＰサーバ(23)から割り当てられたＩＰアドレスとの組合せを記憶しておき、端末機(16)から送信される情報パケットの中に含まれる発信元ＩＰアドレスと、該パケットを受信する下流ポート(33)のＭＡＣアドレスとの組合せが、記憶した組合せと異なる場合には、該パケットの中央ハブ(13)への送信を阻止するＭＡＣフィルタリング機能を有している。

【００１９】上記構成のネットワークシステム(10)における統合サーバ(14)の動作を図３～図７に沿って説明する。端末機(16)からＤＨＣＰ要求を受け取った場合には、図３に示すように、ルータ(20)は、該ＤＨＣＰ要求をＤＨＣＰサーバ(23)に転送し（ステップＳ10）、ＤＨＣＰサーバ(23)からＩＰアドレスを受け取る（ステップＳ11）。そして、該ＩＰアドレスをＤＨＣＰ要求のあった端末機(16)のＭＡＣアドレスに転送して（ステップＳ12）、ＤＨＣＰ要求に関する処理を終了する。

【００２０】端末機(16)が認証ツールを起動して、端末機(16)から認証要求を受け取った場合には、図４に示すように、ルータ(20)は、該認証要求を認証サーバ(24)に転送し（ステップＳ20）、認証サーバ(24)による認証が行なわれる（ステップＳ21）。該認証の具体的な方法については後述する。認証サーバ(24)による認証が成功しなかった場合には、ステップＳ21に戻り、成功した場合には、以下のステップを実行する（ステップＳ22）。認証サーバ(24)からの制御により、ルータ(20)は、成功した端末機(16)のＩＰアドレスを用いて、該端末機(16)から、該端末機(16)の所属するＶＬＡＮの外部のネットワーク、すなわち、各種サーバ(21)、他のＶＬＡＮまたは外部ネットワーク(15)へのアクセスを許可する（ステップＳ23）。このとき、認証サーバ(24)に記憶した前記アクセス制限情報に基づいて、アクセス可能な範囲を制限することもできる。そして、ルータ(20)は、認証サーバ(24)から送られた認証成功ページを端末機に転送して（ステップＳ24）、認証要求に関する処理を終了する。

【００２１】端末機(16)から、各種サーバ(21)、他の端末機(16)、または外部ネットワーク(15)に向けて送信された情報パケットをルータ(20)が受け取った場合には、

図５に示すように、ルータ(20)は、情報パケットに含まれる発信元ＩＰアドレスが認証済みであるか否かを判断し（ステップＳ30）、認証済みでは無い場合には、情報パケットの送信が阻止される。この場合、ルータ(20)は、該情報パケットを破棄し、返信し、認証サーバ(24)に転送し、または該情報パケットを破棄して認証サーバ(24)に通知してもよい。

【００２２】認証済みの場合には、ルータ(20)は、情報パケットに含まれる宛先ＩＰアドレスから、該情報パケットが外部ネットワーク(15)を宛先とするものかどうかを判断する（ステップＳ31）。ネットワークシステム(10)への送信の場合には、発信元のＩＰアドレスに対するアクセス可能範囲に、ネットワークシステム(10)が含まれているか否かを判断する（ステップＳ32）。含まれない場合には、前述と同様に情報パケットの送信が阻止され、含まれる場合には、該情報パケットを宛先ＩＰアドレスへ転送する（ステップＳ33）。外部ネットワーク(15)への送信の場合には、発信元となる端末機(16)のＩＰアドレスと宛先となる外部ネットワーク(15)のＩＰアドレスを記憶すると共に、ＮＡＴ機能により、発信元ＩＰアドレスを、ルータ(20)が有するグローバルＩＰアドレスに変換し、前記情報パケットを外部ネットワークへ転送して（ステップＳ34）、情報パケットの転送処理を終了する。

【００２３】外部ネットワーク(15)から情報パケットを受け取った場合には、図６に示すように、ルータ(20)は、図５のステップＳ34にて記憶した端末機(16)および外部ネットワーク(15)のＩＰアドレスを参照し、該情報パケットに含まれる外部ネットワーク(15)の発信元ＩＰアドレスに送信した端末機のプライベートＩＰアドレスを検索する（ステップＳ40）。該当するプライベートＩＰアドレスが見つからなかった場合には（ステップＳ41）、前記情報パケットを破棄するか、または発信元に返信し、該当するプライベートＩＰアドレスが見つかった場合には、見つかったＩＰアドレスに前記情報パケットを転送して（ステップＳ42）、外部ネットワーク(15)からの情報パケットの転送処理を終了する。

【００２４】切断監視サーバ(25)が端末機(16)の切断を検知した場合には、切断監視サーバ(25)からの指示により、図７に示すように、ＤＨＣＰサーバ(23)は、該端末機(16)が利用していたＩＰアドレスを解放し、ルータ(20)は、該ＩＰアドレスが利用不能となるように設定され（ステップＳ50）、部門ハブ(12)は、該端末機(16)が利用していたポートのＭＡＣフィルタリングを中止するように設定されて（ステップＳ51）、端末機の切断処理を終了する。

【００２５】次に、端末機(16)における動作の流れを図８～図９に沿って説明する。まず、端末機(16)を情報コンセント(11)に接続して（ステップＳ80）、ＩＰアドレスを割り当てるようにＤＨＣＰ要求を送信する（ステップＳ81）。このとき、該ＤＨＣＰ要求は、ルータ(20)を介してＤＨＣＰサーバ(23)に送信される。ＤＨＣＰサーバ(23)は、適当なＩＰアドレスをルータ(20)を介して該端末機に送信することにより、端末機(16)にＩＰアドレスが割り当てられる（ステップＳ82）。

【００２６】次に、認証ツールを起動して認証要求を送信する（ステップＳ83）。このとき、該認証要求は、ルータ(20)を介して認証サーバ(24)に送信される。認証サーバ(24)は、認証ページをルータ(20)を介して該端末機(16)に送信することにより、端末機(16)の画面に認証ページが表示される（ステップＳ84）。次に、利用者は、端末機(16)からＩＤコードおよびパスワードを入力して送信する（ステップＳ85）。このとき、該ＩＤコードおよびパスワードは、ルータ(20)を介して認証サーバ(24)に送信されて、認証が行なわれる。認証に失敗した場合には、再び認証ページをルータ(20)を介して端末機に送信することにより、ステップＳ84に戻る。認証に成功した場合には、認証サーバ(24)は、認証成功のページをルータ(20)を介して端末機(16)に送信することにより、端末機(16)の画面に認証成功のページが表示されて（ステップＳ86）、情報コンセント(11)からのネットワークシステム(10)の利用が開始される（ステップＳ87）。

【００２７】そして、利用者が端末機を情報コンセント(11)から切断して（ステップＳ88）、ネットワークシステム(10)の利用を終了する。このとき、切断監視サーバ(25)は、該切断を検出し（ステップＳ89）、切断監視サーバ(25)からの指示により、ＤＨＣＰサーバ(23)は、該端末機(16)のＩＰアドレスを解放する（ステップＳ90）。

【００２８】従って、本実施形態のネットワークシステム(10)は、ＶＬＡＮ管理方式の設定が可能なスイッチングハブを利用して、図２に示すように、各端末機(16)が、該端末機(16)とルータ(20)からなるＶＬＡＮグループ(40)に所属するように設定される。従って、ネットワークシステム(10)上の端末機(16)(16)どうしは、別々のＶＬＡＮグループ(40)(40)に所属することになるから、該端末機(16)(16)間のセキュリティが向上する。

【００２９】また、或る端末機(16)から、該端末機(16)所属するＶＬＡＮ(40)の外部にパケットを送信する場合には、必ずルータ(20)を介して行われる。従って、ルータ(20)が、認証サーバ(24)の認証により認可されたＩＰアドレスを有する端末機(16)から送信されるパケットのみを、ＶＬＡＮ(40)の外部に送信するように設定されることにより、利用者がネットワークを利用するには、認証を受ける必要性が生じるから、ネットワーク上のセキュリティが向上する。

【００３０】また、ルータ(20)が、端末機(16)におけるＩＰアドレスとＭＡＣアドレスの組合せを記憶し、該組合せに適合しない通信を拒否する機能を有しており、部門ハブ(12)が上記ＭＡＣフィルタリング機能を有してい

るから、或る端末機(16)に割り当てられたＩＰアドレスを他の端末機(16)が利用する、いわゆる「なりすまし」を防止できる。また、ルータ(20)は、ＮＡＴ機能を有するから、外部ネットワーク(15)上からは、グローバルＩＰアドレスを有するルータ(20)のみ参照でき、端末機(16)を直接参照できない。従って、外部ネットワーク(15)から端末機(16)への攻撃を防止できる。また、ＤＨＣＰサーバ(23)は、ＤＨＣＰ要求に対して割り当てたＩＰアドレスを、ＡＲＰブロードキャストではなく、ＤＨＣＰ要求を行なった端末機(16)のＭＡＣアドレスに送るから、他の端末機(16)によるＩＰアドレスの傍受を防止できる。

【００３１】上記実施形態の説明は、本発明を説明するためのものであって、特許請求の範囲に記載の発明を限定し、或いは範囲を減縮する様に解すべきではない。又、本発明の各部構成は上記実施形態に限らず、特許請求の範囲に記載の技術的範囲内で種々の変形が可能であることは勿論である。例えば、ネットワークを物理的又は論理的に区分化できるスイッチングハブとしては、ＶＬＡＮ管理方式の設定が可能なスイッチングハブの他にも、無線のチャンネルにより区分化可能な無線ハブを利用することもできる。

【図面の簡単な説明】

【図１】本発明の実施形態であるネットワークシステムを示す概要図である。

【図２】本実施形態のネットワークシステムにおける論理的な接続を示す概要図である。

【図３】本実施形態の統合サーバにおいてＤＨＣＰ要求

に対する処理動作を示すフローチャートである。

【図４】本実施形態の統合サーバにおいて認証要求に対する処理動作を示すフローチャートである。

【図５】本実施形態の統合サーバにおいて情報パケットの送信に対する処理動作を示すフローチャートである。

【図６】本実施形態の統合サーバにおいて外部ネットワークからの情報パケットの返信に対する処理動作を示すフローチャートである。

【図７】本実施形態の統合サーバにおいて端末機の切断に対する処理動作を示すフローチャートである。

【図８】本実施形態における端末機の動作を示すフローチャートである。

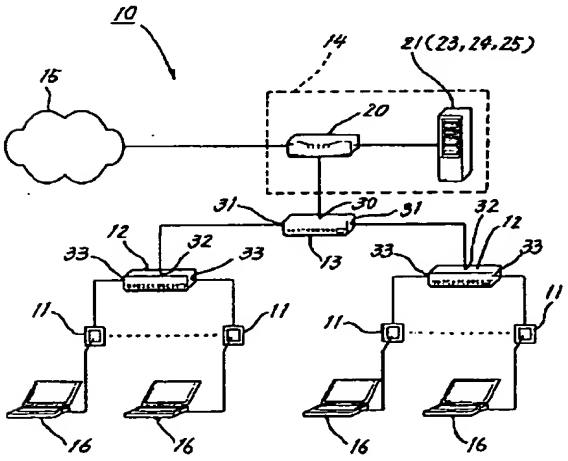
【図９】図８の続きを示すフローチャートである。

【図１０】従来のネットワークシステムを示すブロック図である。

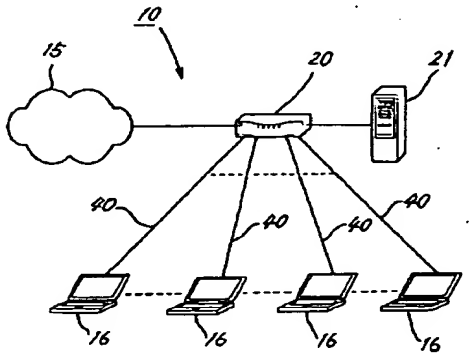
【符号の説明】

(10)　ＴＣＰ／ＩＰネットワークシステム
(11)　情報コンセント
(12)　部門ハブ
(13)　中央ハブ
(15)　外部ネットワーク
(16)　端末機
(20)　ルータ
(23)　ＤＨＣＰサーバ
(24)　認証サーバ
(25)　切断監視サーバ
(33)　部門ハブの下流ポート
(40)　ＶＬＡＮグループ

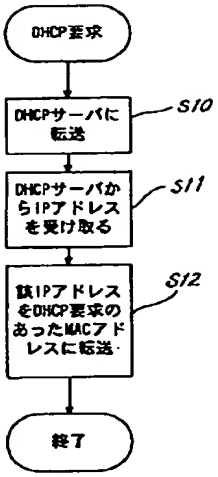
【図１】



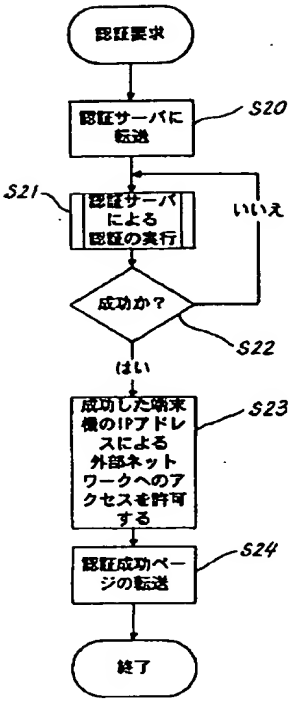
【図２】



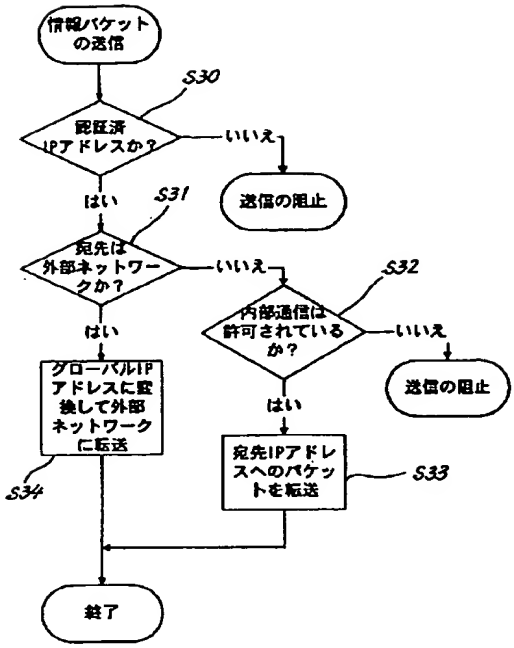
【図３】



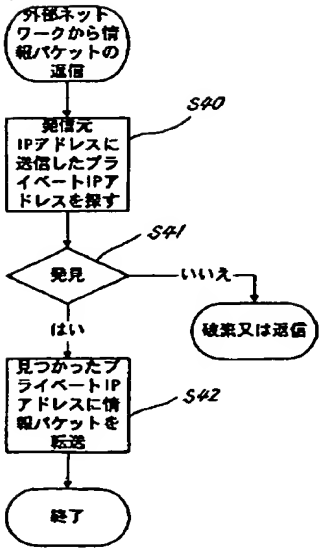
【図４】



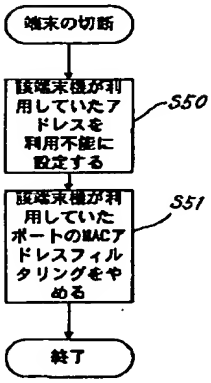
【図５】



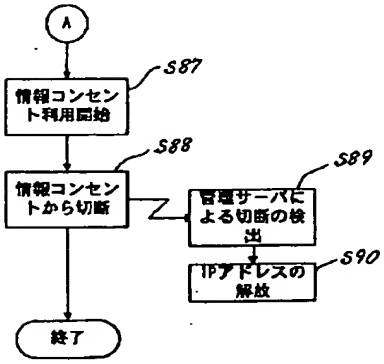
【図６】



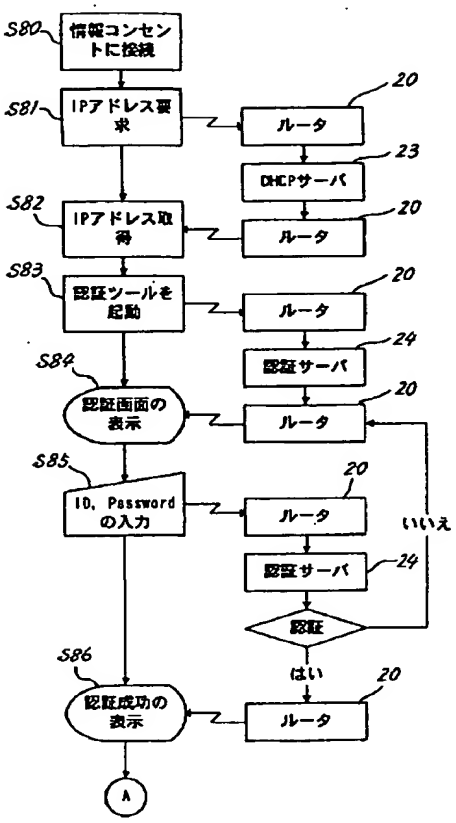
【図７】



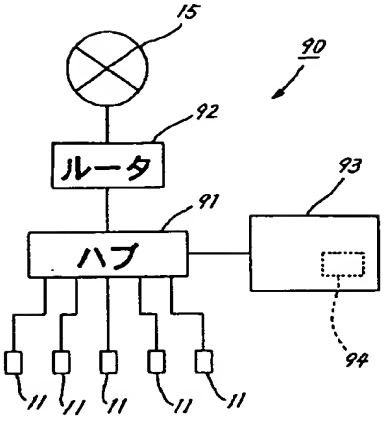
【図９】



【図８】



【図１０】



フロントページの続き

(72)発明者　浅野　善男
滋賀県草津市南笠町448－１－1428
(72)発明者　辻　斉
京都府京都市中京区三条通室町西入衣棚町53－１－805
(72)発明者　藤井　康雄
京都府京都市左京区下鴨宮崎町168－25
(72)発明者　中村　順一
滋賀県大津市下坂本１－47－14

Ｆターム(参考)　5J104 AA07 KA02 MA01 PA07
5K030 GA15 HC14 HD03 HD07 LB05
5K033 CB08 DA05 DA15 DB18 EC03
9A001 CC03 CZ06 JJ25 LL03